POLICY 8.00 BACKUP

Information technology resources will be protected from loss through comprehensive backup techniques and procedures.

PURPOSE:

To minimize the risk that business operations would be disrupted resulting from the loss of data or unavailability of computing resources.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Ensure that all critical computer and network resources can be recovered with minimal impact on required or critical government services.
2. Define the responsibilities of information systems management and users in the protection of information technology resources.
3. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

This policy applies to state agencies, including all persons or organizations that use, process, or store computerized software relevant to official State of Tennessee business.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Maintain backups of all network infrastructure components (such as firewalls, routers, switches, servers, etc.).
2. Install patches, and maintain version control to properly manage software configuration.
3. Maintain network infrastructure component information in electronic and hard copy format, to ensure that in the event of a natural disaster or emergency, systems can be restored to their previous security posture with minimum downtime.
4. Maintain current, machine-readable data in the event that operating data is lost, damaged or destroyed, or corrupted.
5. Maintain sufficient current and historical data in machine-readable form at an off-site environment, to support recovery.
6. Maintain emergency response and disaster recovery procedures.

7. Periodically review critical backup and recovery plans to ensure continued relevance.

Agency

1. Assign an individual the responsibility and authority for administrative oversight for information technology contingency planning, and backup processing and disaster recovery for the agency.
2. Develop, approve and publish agency configuration and backup policies, standards, procedures, and guidelines in accordance with published statewide directives sufficient to ensure a successful statewide information resource recovery.
3. Maintain sufficient current, and historical, data in machine-readable form in a secure off-site to support recovery from the loss of data processing capability.
4. Provide for an agency administrative review of information resource contingency and backup standards, procedures and guidelines in light of technical, environmental, procedural, or statutory changes.

Individual Users/Clients

1. Identify critical local information processing resources, systems, applications and data.
    - Ensure that critical data is stored on the server and not on the local hard drive.
    - End-users should develop contingency plans for local standalone application processing resources.
2. Adhere to statewide and agency policies, standards, procedures and guidelines in support information resource contingency planning and recovery.